

Web 轻网管交换机软件手册

目录

| | |
|-----------------------|----|
| 第一章 手册简介 | 4 |
| 1.1. 目标读者 | 4 |
| 1.2. 手册约定 | 4 |
| 第二章 Web 轻网管功能简介 | 5 |
| 2.1. 功能简介 | 5 |
| 第三章 登录 Web 界面 | 6 |
| 3.1. 登录 | 6 |
| 第四章 系统 | 7 |
| 4.1. 系统信息 | 7 |
| 4.2. IP 设置 | 8 |
| 4.3. 用户设置 | 8 |
| 4.4. 端口设置 | 9 |
| 第五章 POE | 10 |
| 5.1. POE | 10 |
| 第六章 配置 | 11 |
| 6.1. VLAN | 11 |
| 6.1.1. 示例 | 12 |
| 6.2. QoS | 13 |
| 6.2.1. 优先级抉择 | 13 |
| 6.2.2. DSCP 重映射 | 13 |
| 6.2.3. 优先级与队列映射 | 14 |
| 6.2.4. 端口优先级 | 14 |
| 6.2.5. Q 队列权重 | 15 |
| 6.2.6. 示例 1 | 15 |
| 6.2.7. 示例 2 | 17 |
| 6.3. IGMP | 21 |
| 6.3.1. 示例 | 21 |
| 6.4. 端口汇聚 | 22 |
| 6.4.1. 示例 | 23 |
| 6.5. 环路保护 | 26 |
| 6.5.1. 示例 | 26 |
| 6.6. 生成树 | 27 |
| 6.6.1. 示例 | 28 |
| 6.7. 端口镜像 | 30 |
| 6.7.1. 示例 | 30 |
| 6.8. 端口隔离 | 31 |
| 6.8.1. 示例 | 31 |
| 6.9. 带宽控制 | 32 |
| 6.9.1. 示例 | 32 |
| 6.10. 巨型帧 | 33 |
| 6.10.1. 示例 | 33 |
| 6.11. MAC 约束 | 34 |
| 6.11.1. 示例 | 34 |

| | |
|------------------------|----|
| 6.12. 绿色以太网..... | 35 |
| 6.13. 节能以太网（EEE） | 35 |
| 6.14. SNMP | 35 |
| 6.14.1. 示例..... | 36 |
| 第七章 安全 | 38 |
| 7.1. MAC 地址 | 38 |
| 7.1.1. MAC 地址表..... | 38 |
| 7.1.2. MAC 查找..... | 38 |
| 7.1.3. 静态 MAC | 38 |
| 7.2. 广播风暴 | 39 |
| 第八章 监控 | 40 |
| 8.1. 端口统计 | 40 |
| 8.2. 电缆诊断 | 40 |
| 第九章 工具 | 41 |
| 9.1. 固件升级 | 41 |
| 9.2. 配置备份 | 42 |
| 9.3. 复位 | 43 |
| 9.4. 保存 | 43 |
| 9.5. 重启 | 43 |

第一章 手册简介

本手册详细 Web 轻管理交换机软件各项功能的配置方法。请在操作前仔细阅读本手册。

1.1. 目标读者

本手册的目标读者为了解或使用本 Web 轻网管软件功能的人员。

1.2. 手册约定

在本手册中以 8 口交换机为例，展示 Web 界面及软件功能。

用 --> 符号表示菜单的进入顺序，一级功能菜单 --> 二级功能菜单 --> 三级功能菜单，其中，部分功能无二级三级功能菜单。

文中出现的<>尖括号标记文字，表示按钮名称，如<应用>、<apply>。

本手册中使用的特殊图标说明如下：

| | |
|--|-----------------------------------|
| 说明 | 操作内容的描述，进行必要的补充和说明。 |
|  注意 | 提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。 |

第二章 Web 轻网管功能简介

2.1. 功能简介

我司全新开发推出的 Web 轻网管交换机功能软件，支持多种机型形态。提供 VLAN, QoS, RSTP, SNMP, POE 控制, 链路聚合等等功能。

| | |
|--------------------------|-----------------------|
| 首页 | 支持 Logo, 接口面板, 系统信息显示 |
| | |
| 系统 | IP 地址设置, 端口设置, 用户账户 |
| | |
| POE | POE 供电端口控制 |
| | |
| 配置 | VLAN |
| | QOS |
| | IGMP |
| | 链路聚合 |
| | 环路保护 |
| | RSTP |
| | 端口镜像 |
| | 端口隔离 |
| | 带宽控制 |
| | 巨型帧 |
| | MAC 约束 |
| | 绿色以太网 |
| | EEE |
| SNMP (仅支持 V1, 及 V2 部分节点) | |
| | |
| 安全 | MAC 地址 |
| | 广播风暴 |
| | |
| 监控 | 端口统计 |
| | 电缆诊断 |
| | |
| 工具 | 固件升级 |
| | 配置备份 |
| | 复位 |
| | 保存 |
| | 重启 |

说明：带 POE 供电的设备才具有 POE 功能

第三章 登录 Web 界面

3.1. 登录

1. 交换机已正常加电启动，任一端口已与管理 PC 相连。
2. 管理 PC 已至少安装一种以下浏览器：IE 8.0 或以上版本，最新版本的 Chrome，360 浏览器。
3. 管理 PC 的 IP 地址已设为与交换机端口同一网段，即 192.168.200.1 子网掩码为 255.255.255.0。
4. 为保证能更好地体验 Web 界面显示效果，建议将显示器的分辨率调整到 1280×800 或以上像素。
5. 打开浏览器，在地址栏中输入交换机默认管理地址 <http://192.168.200.1> 登录交换机 Web 管理界面。
6. 交换机登录页面如下图所示，输入交换机管理帐号的用户名和密码，出厂默认值均为 admin。



图 1 web 登录界面

7. 登录成功后，web 界面主页显示如下图。



图 2 web 首页

左边导航栏，此为中性软件。没有显示 Logo。右上为机型接口面板。右下为系统基本信息。

第四章 系统

4.1. 系统信息

可以在此查看设备的系统信息，以及设置设备型号。

在导航栏点击：系统 --> 系统信息

| 系统信息 | |
|--------|-------------------|
| 设备型号 | GWGW |
| MAC 地址 | 22:22:22:22:22:22 |
| IP 地址 | 192.168.2.1 |
| 子网掩码 | 255.255.255.0 |
| 网关 | 192.168.2.254 |
| 固件版本 | 1.0.0 |
| 固件日期 | May 17 2022 |
| 硬件版本 | V1.0.0 |
| 运行时间 | 0天0时34分 |

图 3 系统信息

说明：

| | |
|--------|--------------|
| 设备型号 | 显示设备型号 |
| MAC 地址 | 显示设备的 MAC 地址 |
| IP 地址 | 显示设备管理 IP 地址 |
| 子网掩码 | 显示设备子网掩码 |
| 网关 | 显示设备默认网关 |
| 关键版本 | 显示软件版本 |
| 固件日期 | 显示软件版本日期 |
| 硬件版本 | 显示设备硬件版本 |
| 运行时间 | 显示设备运行时间 |

4.2. IP 设置

网络中每一台设备拥有一个 IP 地址，可以通过这个 IP 地址登录管理界面操作交换机。
点击导航栏：系统 --> IP 设置

| IP地址设置 | |
|--------|---------------|
| DHCP设置 | 关闭 |
| IP地址 | 192.168.2.1 |
| 子网掩码 | 255.255.255.0 |
| 网关 | 192.168.2.254 |

Apply

图 4 IP 地址设置

说明：

DHCP 设置 选择开启或禁用 DHCP 功能。

禁用：选择禁用，需手动输入 IP 地址、子网掩码和默认网关。

启用：选择启用，交换机会从 DHCP 服务器获取网络参数。

IP 地址 设置设备的 IP 地址。

子网掩码 设置设备的子网掩码。

默认网关 设置设备的默认网关地址。

点击<Apply> 系统管理 IP、子网掩码、网关将被修改为设定值。

4.3. 用户设置

可以在此修改登录时使用的用户名和密码。

点击导航栏：系统 --> 用户账户

| 用户账户 | |
|------|-------|
| 用户名 | admin |
| 新密码 | |
| 新密码 | |

应用

图 5 用户账户设置

说明：

用户名 设置登录交换机的用户名。用户名长度不能大于 16 个字符，且只能使用数字、英文字母和下划线。

新密码 重新设置登录交换机的密码。新密码长度不能大于 16 个字符，且只能使用数字、英文字母和下划线。确认 2 次输入的密码一样。

注意： 修改密码后请重新刷新页面。

4.4. 端口设置

可以在此修改端口名字，状态，双工速度，流控。

点击导航栏：系统 --> 端口设置

端口设置

| 端口 | 名字 | 状态 | 速度/双工 | 流控 |
|-----|----|----|-------|----|
| 口 1 | | | | |
| 口 2 | | | | |
| 口 3 | | | | |
| 口 4 | | 打开 | 自动 | 关闭 |
| 口 5 | | | | |
| 口 6 | | | | |

应用

| 端口 | 名字 | 状态 | 速度/双工 | | 流控 | |
|-----|----|----|-------|--------|----|----|
| | | | 配置 | 实际 | 配置 | 实际 |
| 口 1 | | 打开 | 自动 | 掉线 | 关闭 | 关闭 |
| 口 2 | | 打开 | 自动 | 1000双工 | 关闭 | 关闭 |
| 口 3 | | 打开 | 自动 | 掉线 | 关闭 | 关闭 |
| 口 4 | | 打开 | 自动 | 掉线 | 关闭 | 关闭 |
| 口 5 | | 打开 | 自动 | 掉线 | 关闭 | 关闭 |
| 口 6 | | 打开 | 自动 | 掉线 | 关闭 | 关闭 |
| 口 7 | | 打开 | 自动 | 掉线 | 关闭 | 关闭 |
| 口 8 | | 打开 | 自动 | 掉线 | 关闭 | 关闭 |

图 6 端口设置

说明：

名字 设置端口别名。

端口 打开关闭，若打开端口，则端口可以正常转发报文。

速度/双工 可选择 10M/Half, 10M/Full, 100M/Half, 100M/Full, 自动。模式选择为自动时，速率和双工将由协商决定

流控功能 打开关闭，打开流控功能，可以控制调节各端口数据包转发的速率，避免出现拥塞

更改设置后需点击端口设置，刷新显示状态

注意：半双工模式下实际会打开流控功能

第五章 POE

5.1. POE

显示 POE 端口消耗的总功率

点击导航栏：POE -->系统



图 7 POE 消耗的总功率

可以在此设置 PSE 端口状态(支持 POE 供电功能的设备才有此设置)

点击导航栏：POE --> 端口



图 8 PSE 端口设置

说明：

端口 可选择多个端口

状态 在打开状态下能正常供电。

电源开/关 显示当前工作状态

功率 显示端口输出功率

电压 显示 PSE 端口供电电压

电流 显示 PSE 端口供电电流

第六章 配置

6.1. VLAN

VLAN (Virtual Local Area Network, 虚拟局域网) 是将一个物理的 LAN 在逻辑上划分成多个广播域的通信技术,这种技术通过在局域网数据帧上定义扩展字段, 来对物理网络进行逻辑上的分割, 从而限定局域网数据帧的转发范围, 缩小广播域。VLAN 技术主要应用于交换机、路由器和交换机等网络设备中。

点击导航栏: 配置 --> VLAN --> 静态 VLAN



图 9 静态 VLAN

点击导航栏: 配置 --> VLAN --> VLAN 设置



图 10 VLAN 设置

VLAN 由 VLAN ID 区分, 所有到达端口的 Untagged 数据包都会被标记端口 PVID 的 Tag。

说明:

需先设置 VLAN ID 再设置端口 VID

静态 VLAN 设置 VLAN ID, 取值范围 1-4094。

Untagged 端口 若选择为 Untagged 端口, 则输出的数据帧不带 tag 信息。

Tagged 端口 若选择为 Tagged 端口, 则输出的数据帧带tag 信息。

没有成员端口 选择后, 表示该端口不属于 VLAN 的成员端口。

注意: 删除 VLAN 前, 需先设置使用了此 VLAN 的端口的 VID 为 1, 再删除此 VLAN。

6.1.1. 示例

将交换机 1、2、3 端口设置位 VLAN10， 4、5、6、7 端口设置位 VLAN20,端口 8 作为上联口分别加入 VLAN10， VLAN20。同时 VLAN1 包含所有端口。这样 VLAN10， VLAN20 的端口数据包都能转发到 8 端口。如下图所示



图 11 VLAN 表设置

设置好 VLAN 表后，还需要设置端口 VID。将端口 1、2、3 的端口 VID 设置为 10，端口 4、5、6、7 的端口 VID 设置为 20，端口 8 的 VID 设置为默认 1。这样 8 端口的数据能转发到所有端口。结果如下列图所示

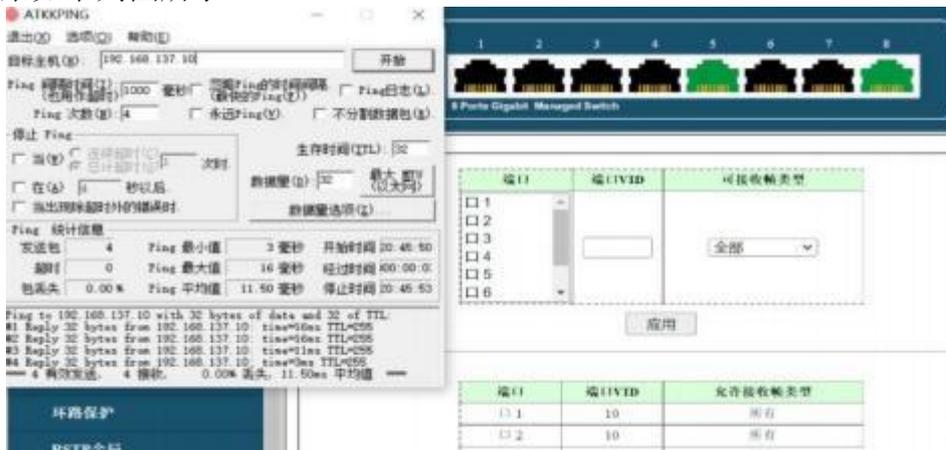


图 12 设置 VLAN 后端口 5/8 ping 通



图 13 设置 VLAN 后端口 2/8 ping 通



图 14 设置 VLAN 后端口 2/6 ping 不通
实现了端口 1、2、3 与端口 4、5、6、7 的隔离，与上联口 8 都能通信。

6.2. QoS

QoS（服务质量）功能用于优化网络性能，提供更好的网络服务体验。交换机基于端口、802.1P、DSCP 优先级模式。

6.2.1. 优先级抉择

点击导航栏：配置 --> QOS --> 优先级抉择



图 15 优先级选择设置

说明：

优先级选择 设置优先级源的优先级，根据最高优先级的优先级源指定帧的传输队列。

6.2.2. DSCP 重映射

DSCP 给了 IP DSCP 字段一个推荐的定义。IP 数据包根据 DSCP 值（0-63）映射到 8 个优先级。

点击导航栏：配置 --> QOS --> DSCP 重映射

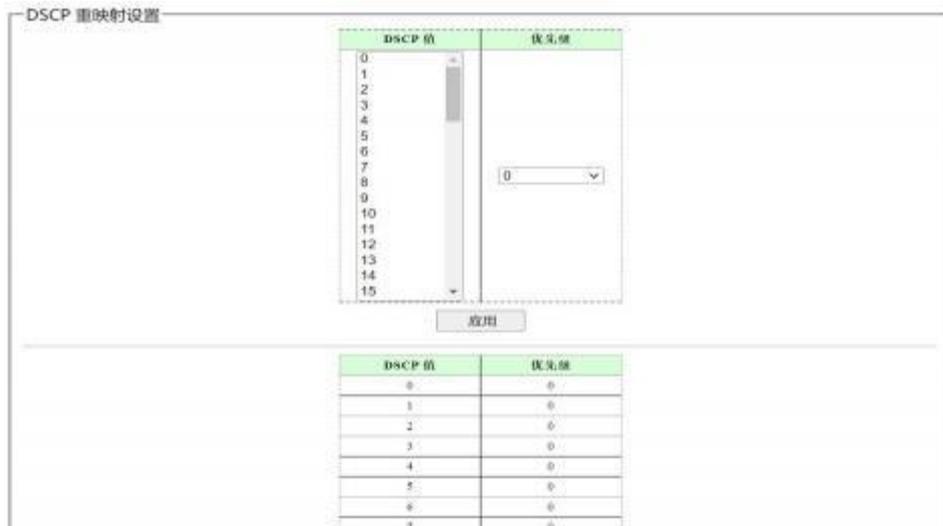


图 16 DSCP 优先级映射

说明：

将 DSCP 值映射到内部的优先级

6.2.3. 优先级与队列映射

将不同优先级映射到不同队列（4 个队列）

点击导航栏：配置 --> QOS --> 优先级到队列

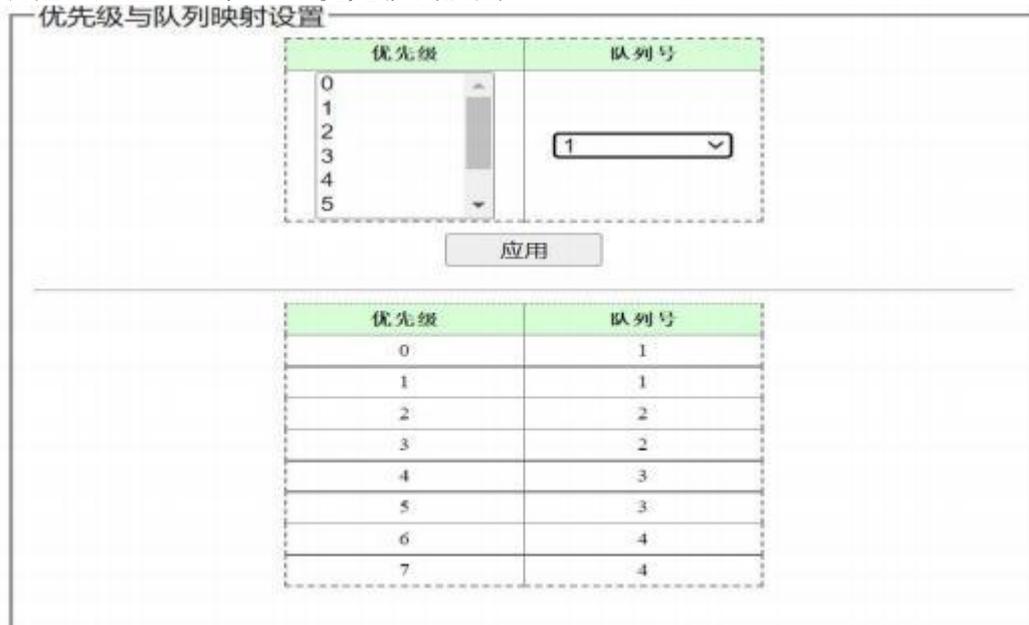


图 17 优先级队列映射

6.2.4. 端口优先级

基于入端口这些包被映射到 8 个不同的优先级级别。

点击导航栏：配置 --> QOS --> 端口优先级

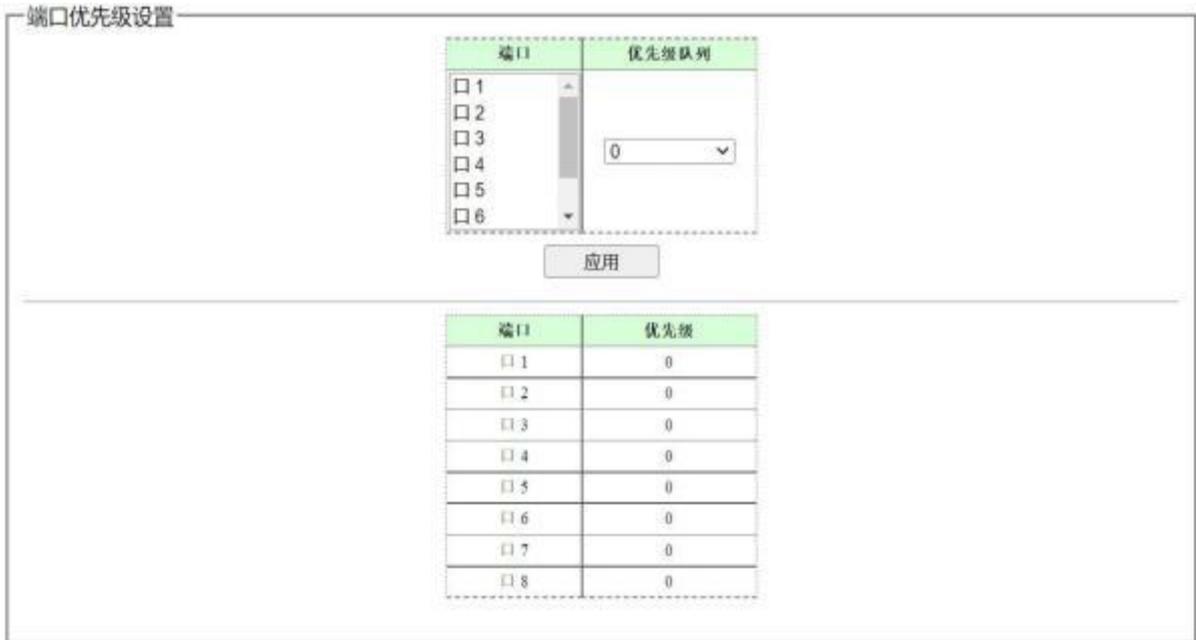


图 18 端口优先级设置

6.2.5. Q 队列权重

设置队列权重，使不同队列获得不同的调度优先级。

点击导航栏：配置 --> QOS --> Q 队列权重



图 19 Q 队列权重

6.2.6. 示例 1

端口优先级示例

1、按如下拓扑连接设备。

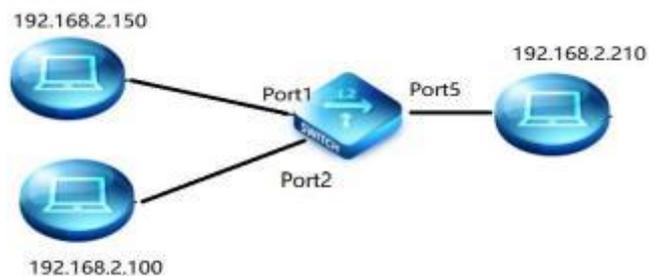


图 20 连接拓扑

2、便于测试将端口 1、2 设置为 10M Full。端口 5 限速为 15Mbps

端口设置

| 端口 | 名字 | 状态 | 速率/双工 | 流控 |
|----------------------------|----|----|-------|----|
| <input type="checkbox"/> 1 | | | | |
| <input type="checkbox"/> 2 | | | | |
| <input type="checkbox"/> 3 | | | | |
| <input type="checkbox"/> 4 | | 打开 | 自动 | 关闭 |
| <input type="checkbox"/> 5 | | | | |
| <input type="checkbox"/> 6 | | | | |

应用

| 端口 | 名字 | 状态 | 速率/双工 | | 流控 | |
|-----|----|----|-------|---------|----|----|
| | | | 配置 | 实际 | 配置 | 实际 |
| 口 1 | | 打开 | 10 双工 | 10 双工 | 关闭 | 关闭 |
| 口 2 | | 打开 | 10 双工 | 10 双工 | 关闭 | 关闭 |
| 口 3 | | 打开 | 自动 | 协商 | 关闭 | 关闭 |
| 口 4 | | 打开 | 自动 | 协商 | 关闭 | 关闭 |
| 口 5 | | 打开 | 自动 | 1000 双工 | 关闭 | 关闭 |
| 口 6 | | 打开 | 自动 | 协商 | 关闭 | 关闭 |
| 累 1 | | 打开 | 自动 | 协商 | 关闭 | 关闭 |

图 21 端口 1/2 设置

带宽设置

| 端口 | 类型 | 状态 | 速率(Kbit/秒) |
|----------------------------|----|----|--------------------------------------|
| <input type="checkbox"/> 1 | | | |
| <input type="checkbox"/> 2 | | | |
| <input type="checkbox"/> 3 | 入口 | 关闭 | Unlimited (3-1000000, multiple of 8) |
| <input type="checkbox"/> 4 | | | |
| <input type="checkbox"/> 5 | | | |
| <input type="checkbox"/> 6 | | | |

应用

| 端口 | 入口 (Kbit/秒) | 出口 (Kbit/秒) |
|-----|-------------|-------------|
| 口 1 | 不限制 | 不限制 |
| 口 2 | 不限制 | 不限制 |
| 口 3 | 不限制 | 不限制 |
| 口 4 | 不限制 | 不限制 |
| 口 5 | 15360 | 15360 |
| 口 6 | 不限制 | 不限制 |
| 累 1 | 10240 | 10240 |

图 22 端口 5 限速

3、打开测试软件，测试未设置端口优先级时的端口 1、2 发送速率。端口 1、2 的发送速率在不断变化。



图 23 未设置端口优先级时，端口 1/2 带宽分布

4、设置端口 1 优先级为 6，端口 2 优先级为 2。

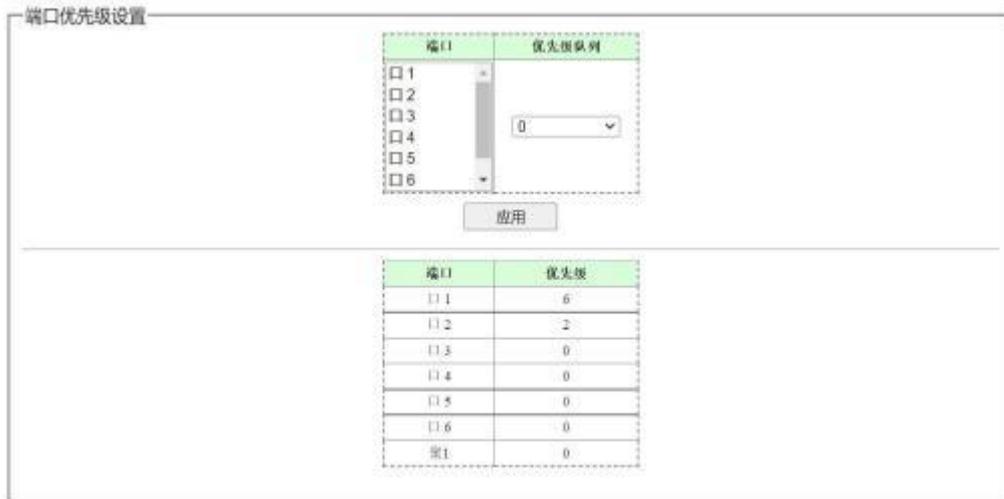


图 24 端口优先级设置

4、打开测试软件，测试设置端口优先级后的端口 1、2 的发送速率。端口 1 速率近 10M bps，端口 2 只有 5Mbps。

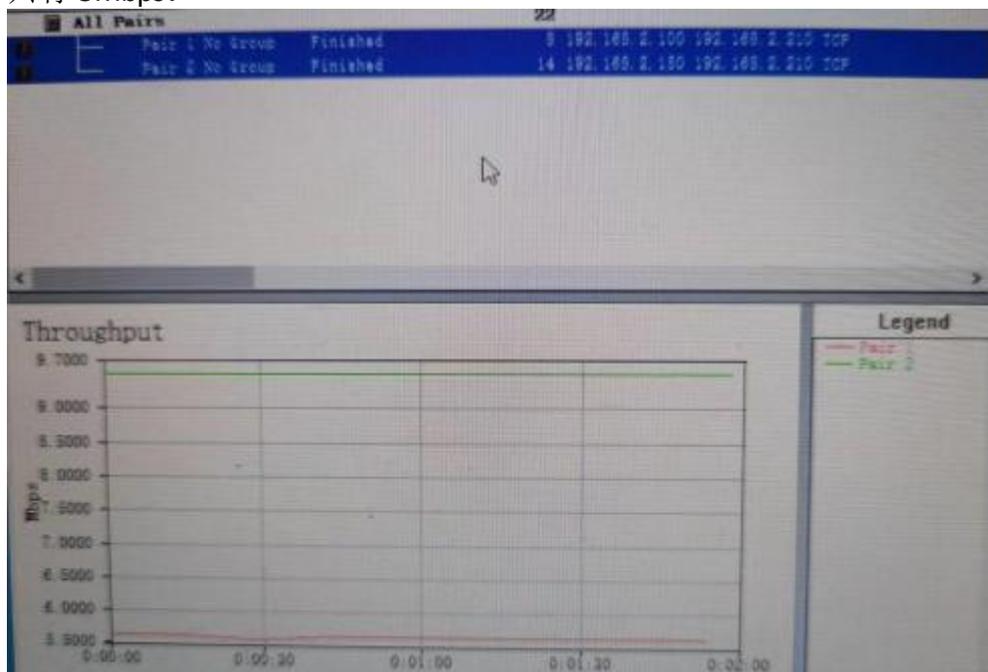


图 25 设置端口优先级后，端口带宽分布

6.2.7. 示例 2

队列权重示例

1、按示例 1 拓扑连接，端口 1 接 IP 为 192.168.2.100 的设备，端口 8 接 IP 为 192.168.2.150 的设备，端口 5 接 192.168.2.210 设备。

2、设置优先级与队列映射。

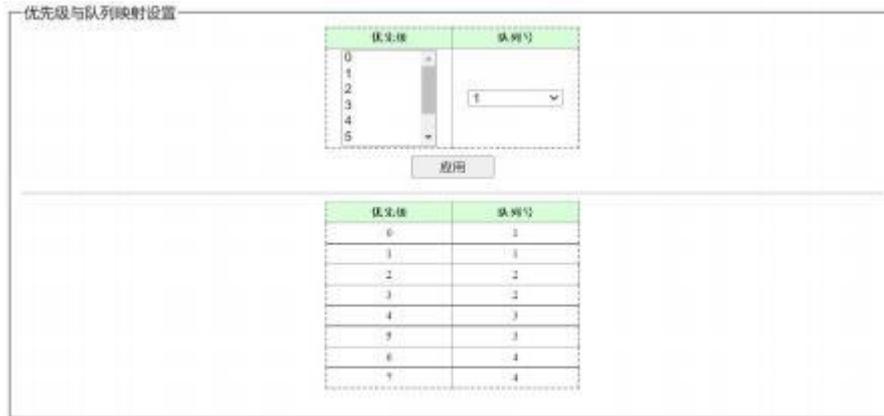


图 26 优先级与队列映射

3、设置端口优先级

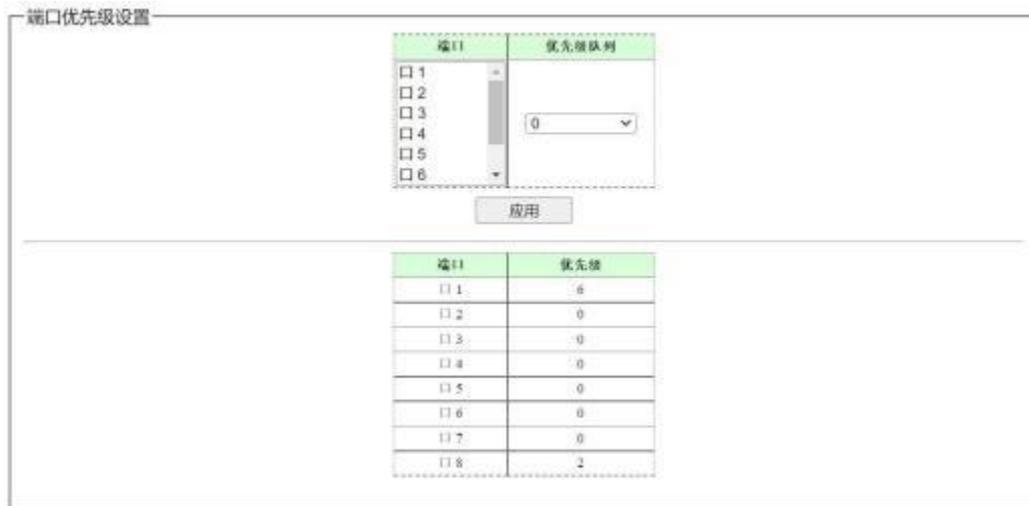


图 27 端口优先级

4、未设置队列权重，默认严格优先级。



图 28 默认严格优先级设置

5、打开测试软件，打流测试。结果如下图，端口 1 发送速率约为 980Mbps，端口 8 发送速率约为 10Mbps。



图 29 未设置队列权重结果

5、修改队列权重如下图。



图 30 队列权重设置

6、重新测试结果如下图所示，端口 8 发送速率变成 880Mbps，端口 1 发送速率变成 121 Mbps。

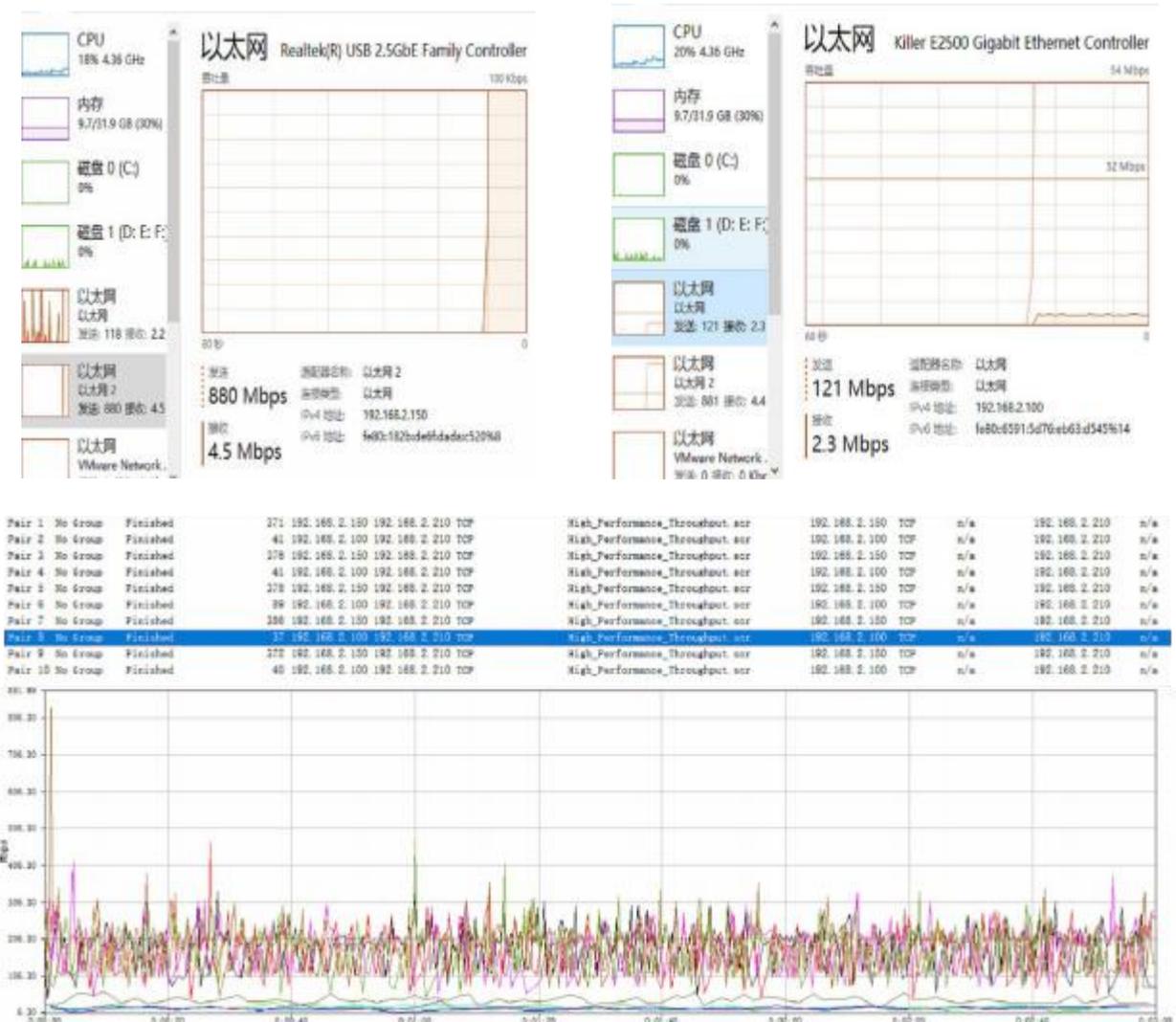


图 31 设置队列权重后测试结果

6.3. IGMP

IGMP 是一种网络组播协议，用来在主机和组播路由器之间建立和维护组播成员关系。IGMP Snooping 通过侦听和分析组播设备与主机之间发送的组播报文来控制这些组播组，有利于抑制二层网络中不必要的组播数据转发，节省网络带宽。

点击导航栏：配置 --> IGMP



图 32 IGMP 设置

说明：

IGMP 使能设置 选择启用或禁用 IGMP 侦听功能。

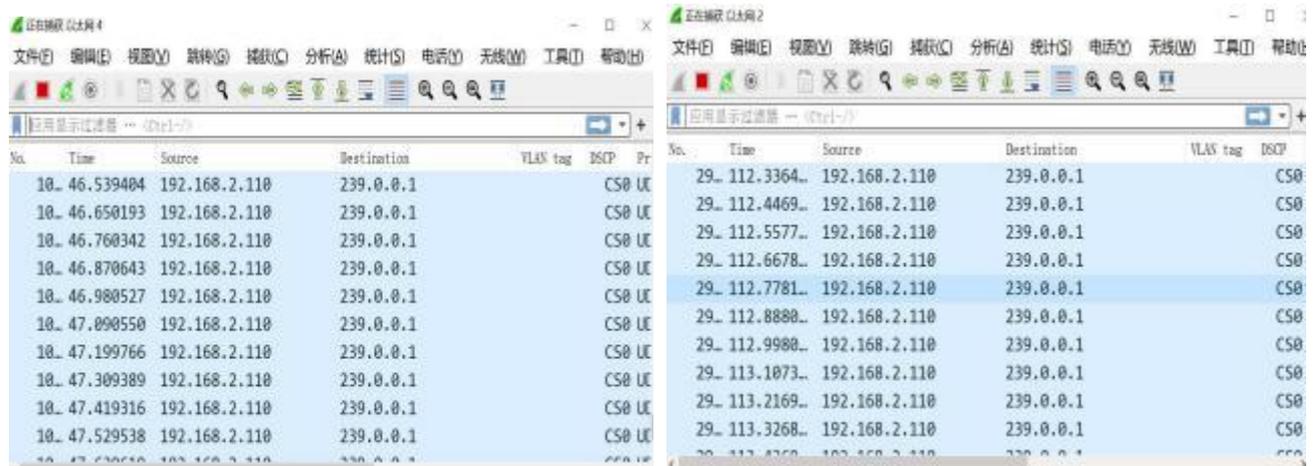
IP 地址 查看组播 IP 地址

端口 查看组播组端口列表

VID 查看组播组对应 VLAN ID

6.3.1. 示例

未开启 IGMP 功能时组播报文在交换机广播



打开 IGMP 功能后，显示出组播地址表，组播报文只在对应组播成员端口转发

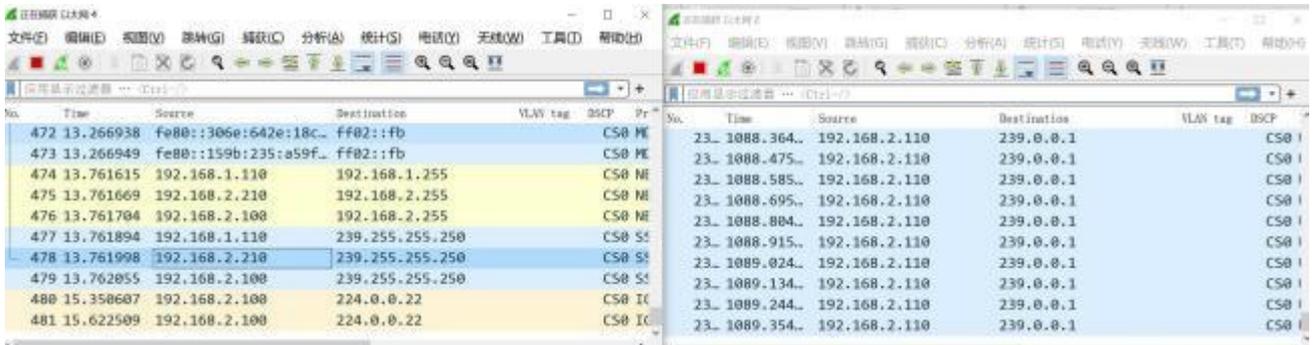




图 33 组播地址表

说明:

- IP 地址 组播 IP
- 端口 组播端口
- VID VLAN ID

6.4. 端口汇聚

端口汇聚 (trunk) 是将一组物理接口捆绑在一起作为一个逻辑接口来增加带宽和可靠性的一种方法, 设置汇聚的端口配置需要一样。

在有以下需求时, 可通过配置链路聚合实现:

当两台交换机设备之间通过一条链路连接可靠性不满足要求时。

点击导航栏: 配置 --> 链路聚合设置

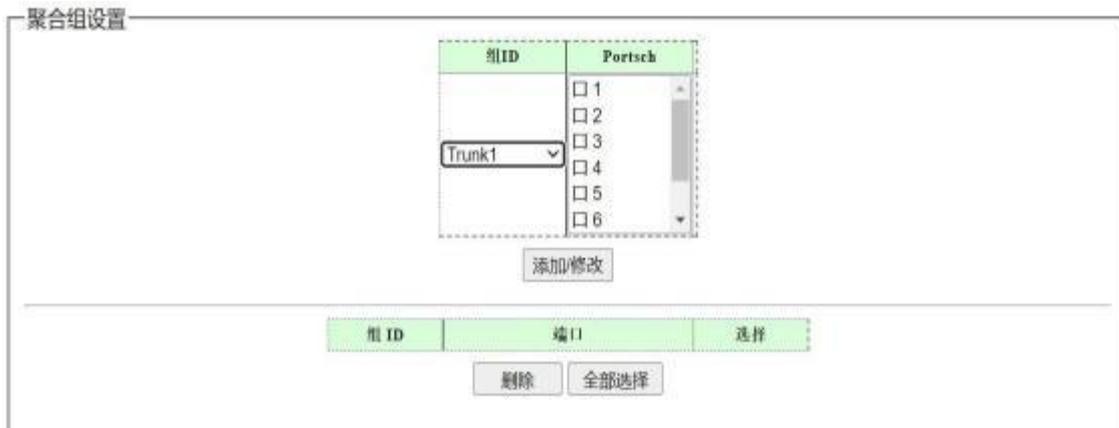


图 34 链路聚合设置

说明:

组 ID 汇聚组 ID。

端口 属于汇聚组的物理端口

属于同一个汇聚组中的成员端口必须有一致的配置。

注意: trunk 1 支持 1~4 口, trunk 2 支持 5~8 口, trunk3 (10 口交换机) 支持 9~10 口

6.4.1. 示例

设置交换机端口聚合功能，测试拓扑如下图所示。



图 35 测试拓扑

1、设置交换机 1 的端口 7、8，自适应。

端口设置

| 端口 | 名字 | 状态 | 速率/双工 | 策略 |
|----|----|----|-------|----|
| 口1 | | | | |
| 口2 | | | | |
| 口3 | | 打开 | 自协商 | 关闭 |
| 口4 | | | | |
| 口5 | | | | |
| 口6 | | | | |

应用

| 编号 | 名字 | 状态 | 速率/双工 | | 策略 | |
|----|----|----|-------|--------|----|----|
| | | | 配置 | 实际 | 配置 | 实际 |
| 口1 | | 打开 | 自动 | 协商 | 关闭 | 关闭 |
| 口2 | | 打开 | 自动 | 协商 | 关闭 | 关闭 |
| 口3 | | 打开 | 自动 | 协商 | 关闭 | 关闭 |
| 口4 | | 打开 | 自动 | 1000半工 | 关闭 | 关闭 |
| 口5 | | 打开 | 自动 | 协商 | 关闭 | 关闭 |
| 口6 | | 打开 | 自动 | 协商 | 关闭 | 关闭 |
| 口7 | | 打开 | 自动 | 协商 | 关闭 | 关闭 |
| 口8 | | 打开 | 自动 | 1000半工 | 关闭 | 关闭 |

图 36 端口设置

2、为了方便测试，将端口 7、8 带宽设置为 10240Kbps

带宽设置

| 端口 | 类型 | 状态 | 速率(Kbit/秒) |
|----|----|----|---------------------------------------|
| 口1 | | | |
| 口2 | | | |
| 口3 | 入口 | 关闭 | Unlimited (8-10000000, multiple of 8) |
| 口4 | | | |
| 口5 | | | |
| 口6 | | | |

应用

| 端口 | 入口 (Kbit/秒) | 出口 (Kbit/秒) |
|----|-------------|-------------|
| 口1 | 不限制 | 不限制 |
| 口2 | 不限制 | 不限制 |
| 口3 | 不限制 | 不限制 |
| 口4 | 不限制 | 不限制 |
| 口5 | 不限制 | 不限制 |
| 口6 | 不限制 | 不限制 |
| 口7 | 10240 | 10240 |
| 口8 | 10240 | 10240 |

图 37 带宽设置

3、设置 7、8 端口为聚合口。另一交换机同样设置。

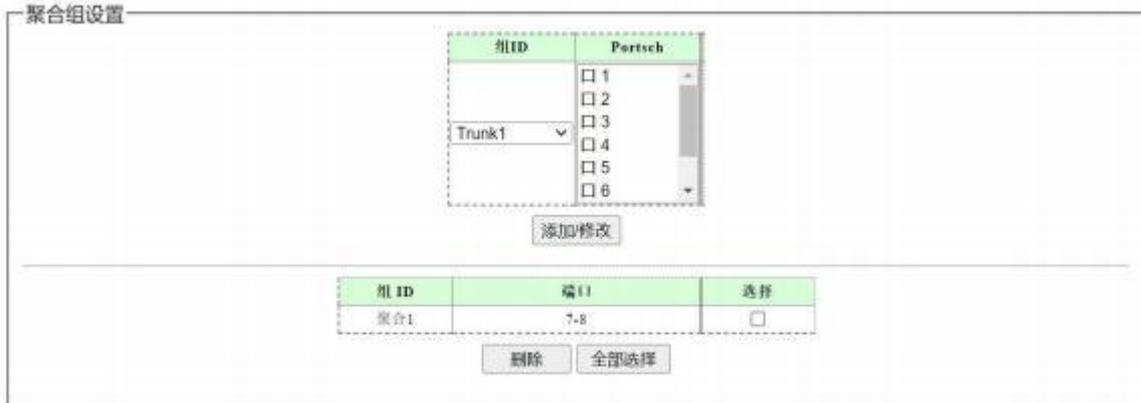


图 38 聚合设置

4、将测试设备按测试拓扑连接。

5、打开测试软件打流测试，先双网线连接查看速率，断开其中一条网线后查看速率变化，再接上断开的网线查看速率变化。结果如下列图所示。



图 39 双网线连接时的速率



图 40 断开一条网线后的速率



图 41 重新接上双网线后的速率

6、根据测试，在单口设置带宽 10Mbps 时，使用端口汇聚功能，提高了网络可靠性，并且增加了带宽。

6.5. 环路保护

环路即交换机下接网络形成环的拓扑结构，环路会造成内网广播风暴，会消耗交换机大量的 CPU 和线路带宽，严重时甚至可以造成设备死机，网络瘫痪。

点击导航栏：配置 --> 环路保护



图 42 环路保护设置

说明:

时间间隔 以该时间间隔为周期监测网络环路

恢复时间 发现环路后，交换机会启动处理机制，会在该时间后端口自动恢复正常。

6.5.1. 示例

1、先将交换机环路检测功能开启，将端口 3、4 用网线连接到另一台交换机形成环路或者自环，出现下图（因为出现环路导致网络瘫痪，不一定刷新出此图），相应环路端口指示灯会慢闪，环路检测并不能预防环路，形成环路后交换机网络将瘫痪



图 43 环路检测

2、开启交换机环路预防，打开所有端口环路预防，将端口 3、4 用网线连接到另一台交换机形成环路。管理主机依然能够 ping 通 192.168.137.10 的设备。



图 44 开启环路预防

6.6. 生成树

以太网交换网络中为了进行链路备份，提高网络可靠性，通常会使用冗余链路。但是使用冗余链路会在交换网络上产生环路，引发广播风暴以及 MAC 地址表不稳定等故障现象，从而导致用户通信质量较差，甚至通信中断。为解决交换网络中的环路问题，提出了生成树协议 STP（Spanning Tree Protocol）。

与众多协议的发展过程一样，生成树协议也是随着网络的发展而不断更新的，从最初的 IEEE 802.1D 中定义的 STP 到 IEEE 802.1W 中定义的快速生成树协议 RSTP（Rapid Spanning Tree Protocol），再到最新的 IEEE 802.1S 中定义的多生成树协议 MSTP。

点击导航栏：配置 --> RSTP 全局 配置 --> RSTP 端口

图 45 生成树全局设置

| 端口 | 状态 | 角色 | 路径开销 | | 优先级 | 点到点 | | 边缘 | |
|-----|----|----|------|---------|-----|-----|----|----|----|
| | | | 设置 | 实际 | | 设置 | 实际 | 设置 | 实际 |
| 口 1 | 转发 | 禁用 | 自动 | 20000 | 128 | 自动 | 否 | 否 | 否 |
| 口 2 | 转发 | 禁用 | 自动 | 2000000 | 128 | 自动 | 否 | 否 | 否 |
| 口 3 | 转发 | 禁用 | 自动 | 2000000 | 128 | 自动 | 否 | 否 | 否 |
| 口 4 | 转发 | 禁用 | 自动 | 20000 | 128 | 自动 | 是 | 否 | 否 |
| 口 5 | 转发 | 禁用 | 自动 | 20000 | 128 | 自动 | 否 | 否 | 否 |
| 口 6 | 转发 | 禁用 | 自动 | 2000000 | 128 | 自动 | 否 | 否 | 否 |
| 口 7 | 转发 | 禁用 | 自动 | 2000000 | 128 | 自动 | 否 | 否 | 否 |
| 口 8 | 转发 | 禁用 | 自动 | 2000000 | 128 | 自动 | 否 | 否 | 否 |

图 46 生成树端口设置

根桥：首先比较交换机的优先级，优先级小的交换机作为根桥交换机；如果优先级都相同，则选择 MAC 地址小的作为根桥交换机。

根端口：在每一个非根桥交换机上选举一个根端口，首先比较交换机端口到达根桥的链路的开销值（越小越优）；如果开销值一样，则比较上行交换机的桥 ID（优先级—>MAC 地址）；如果存在两条链路，则选举上行链路交换机端口号比较小的那一条链路所在的端口成为根端口。

指定端口：在每一段链路上选举一个指定端口（一般根桥的接口都是指定端口）比较在链路两端的交换机的根端口到达根桥的开销，开销小的一边成为指定端口；如果开销一样，则比较链路两端的交换机的桥 ID 大小，桥 ID 小的成为指定端口，对端的端口成为阻塞端口。

阻塞端口：通过以上的选举完成后，链路上的端口没有被选举的成为阻塞端口

6.6.1. 示例

1、点击导航栏：配置 --> 环路保护 开启生成树。



图 47 开启生成树

2、点击导航栏：配置 --> RSTP 全局 设置交换机优先级。



图 48 RSTP 全局设置

3、点击导航栏：配置 --> RSTP 端口 设置路径开销。



图 49 RSTP 端口设置

4、用 3 台交换机组如下图拓扑。

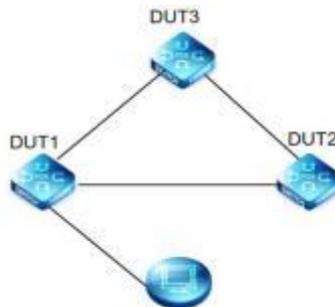


图 50 测试拓扑

5、交换机经过计算，会自动选举出根交换机，根端口，阻塞端口。

生成树设置

| | |
|----------|-------------------|
| 生成树状态 | 打开 |
| 版本 | RSTP |
| 优先级 | 32768 |
| 最大老化时间 | 20 (6-40 Sec) |
| 欢迎时间 | 2 (1-10 Sec) |
| 转发延时(th) | 15 (4-30 Sec) |
| 根优先级 | 32768 |
| 根MAC地址 | 00:23:79:00:23:79 |
| 根路径消耗 | 2000000 |
| 根端口 | 11 5 |
| 根最大老化时间 | 20 Sec |
| 根欢迎时间 | 2 Sec |
| 根转发延时 | 15 Sec |

应用

生成树设置

| 端口 | 路径开销 | 优先级 | 点到点 | 边缘 |
|----------------------------|---|-----|-----|----|
| <input type="checkbox"/> 1 | <input type="text" value="0"/> (1-200000000), 0 = Auto | 128 | 自动 | 否 |
| <input type="checkbox"/> 2 | | | | |
| <input type="checkbox"/> 3 | | | | |
| <input type="checkbox"/> 4 | | | | |
| <input type="checkbox"/> 5 | | | | |
| <input type="checkbox"/> 6 | | | | |

应用

| 端口 | 状态 | 角色 | 路径消耗 | | 优先级 | 点到点 | | 边缘 | |
|-----|----|----|------|---------|-----|-----|----|----|----|
| | | | 设置 | 实际 | | 设置 | 实际 | 设置 | 实际 |
| 口 1 | 禁用 | - | 自动 | - | 128 | 自动 | - | 否 | - |
| 口 2 | 禁用 | - | 自动 | - | 128 | 自动 | - | 否 | - |
| 口 3 | 禁用 | - | 自动 | - | 128 | 自动 | - | 否 | - |
| 口 4 | 转发 | 根 | 自动 | 2000000 | 128 | 自动 | 否 | 否 | 否 |
| 口 5 | 禁用 | - | 自动 | - | 128 | 自动 | - | 否 | - |
| 口 6 | 禁用 | - | 自动 | - | 128 | 自动 | - | 否 | - |
| 口 7 | 阻塞 | 备用 | 自动 | 2000000 | 128 | 自动 | 否 | 否 | 否 |
| 口 8 | 禁用 | - | 自动 | - | 128 | 自动 | - | 否 | - |

图 51 RSTP 结果

6、断开根端口，更改拓扑，交换机重新选择根端口。

| 端口 | 状态 | 角色 | 路径消耗 | | 优先级 | 点到点 | | 边缘 | |
|-----|----|----|------|---------|-----|-----|----|----|----|
| | | | 设置 | 实际 | | 设置 | 实际 | 设置 | 实际 |
| 口 1 | 禁用 | - | 自动 | - | 128 | 自动 | - | 否 | - |
| 口 2 | 禁用 | - | 自动 | - | 128 | 自动 | - | 否 | - |
| 口 3 | 禁用 | - | 自动 | - | 128 | 自动 | - | 否 | - |
| 口 4 | 禁用 | - | 自动 | - | 128 | 自动 | - | 否 | - |
| 口 5 | 禁用 | - | 自动 | - | 128 | 自动 | - | 否 | - |
| 口 6 | 禁用 | - | 自动 | - | 128 | 自动 | - | 否 | - |
| 口 7 | 转发 | 根 | 自动 | 2000000 | 128 | 自动 | 否 | 否 | 否 |
| 口 8 | 禁用 | - | 自动 | - | 128 | 自动 | - | 否 | - |

图 52 拓扑更改

6.7. 端口镜像

端口镜像是把交换机指定端口的报文复制给目的端口；其中被复制的端口称为源端口，复制的端口称为目的端口。目的端口会接入数据检测设备，用户利用这些设备分析目的端口接收到的报文，进行网络监控和故障排除

点击导航栏：配置 --> 端口镜像



图 53 端口镜像

说明：

镜像方向 被镜像端口的数据流方向（入方向，出方向，双方向）

6.7.1. 示例

端口 1 连接 IP 地址 192.168.137.10 的设备，端口 5 连接 192.168.137.251 设备，端口 8 连接管理主机，设置端口 8 为监控端口，端口 1 为被监控端口。在管理主机使用 Wireshark 抓包。可以发现在 Wireshark 中抓取到 ping 包如图所示



图 54 端口镜像设置

| No. | Time | Source | Destination | VLAN tag | DSCP | Protocol | Length | Info |
|------|------------|-----------------|-----------------|----------|------|----------|--------|----------------------------|
| 55.. | 381.3611.. | 192.168.137.10 | 192.168.137.251 | | | CS0 ICMP | 74 | Echo (ping) reply id=0x0 |
| 55.. | 381.3611.. | 192.168.137.10 | 192.168.137.251 | | | CS0 ICMP | 74 | Echo (ping) reply id=0x0 |
| 55.. | 381.3648.. | 192.168.137.10 | 192.168.137.251 | | | CS0 ICMP | 74 | Echo (ping) reply id=0x0 |
| 55.. | 381.3648.. | 192.168.137.10 | 192.168.137.251 | | | CS0 ICMP | 74 | Echo (ping) reply id=0x0 |
| 55.. | 382.0126.. | 192.168.137.251 | 192.168.137.10 | | | CS0 ICMP | 74 | Echo (ping) request id=0x0 |
| 55.. | 382.0127.. | 192.168.137,1 | 192.168.137.251 | | | CS0 ICMP | 102 | Redirect (Redir |
| 55.. | 382.0127.. | 192.168.137.251 | 192.168.137.10 | | | CS0 ICMP | 74 | Echo (ping) request id=0x0 |
| 55.. | 382.0128.. | 192.168.137.251 | 192.168.137.10 | | | CS0 ICMP | 74 | Echo (ping) request id=0x0 |
| 55.. | 382.0128.. | 192.168.137.251 | 192.168.137.10 | | | CS0 ICMP | 74 | Echo (ping) request id=0x0 |
| 55.. | 382.0130.. | 192.168.137.251 | 192.168.137.10 | | | CS0 ICMP | 74 | Echo (ping) request id=0x0 |
| 55.. | 382.0130.. | 192.168.137.251 | 192.168.137.10 | | | CS0 ICMP | 74 | Echo (ping) request id=0x0 |

图 55 Wireshark 抓包结果

6.8. 端口隔离

点击导航栏：配置 --> 端口隔离

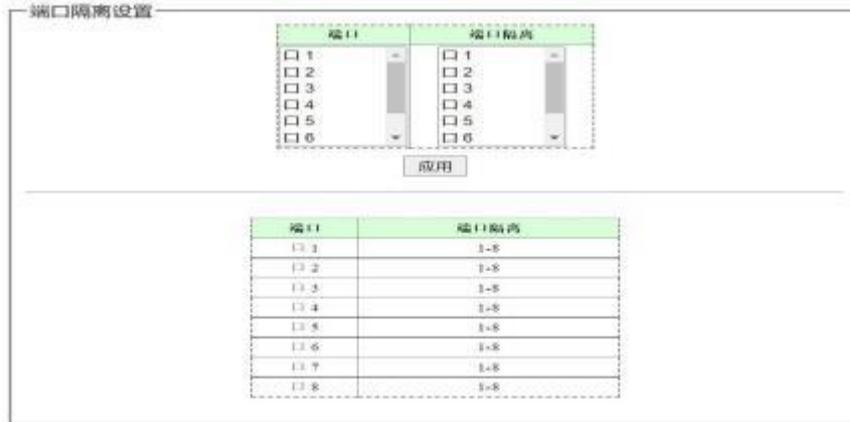


图 56 端口隔离

说明：

端口 源端口

端口隔离 可转发端口

为源端口配置转发端口，源端口接收到的数据包，不能转发到不在转发端口中的端口。

6.8.1. 示例

设置端口 1 与端口 2、3 能相互转发数据包，端口 1 数据不能转发到其他端口（端口 4-8）。在 web 端口选择口 1，在端口隔离多选口 1、2、3。Ping 包测试，7 口与 1 口 Ping 包不通如下图。



图 57 7 口 ping 包结果

3 端口与 1 端口 ping 包能 ping 通，如下图。



图 58 3 口 ping 包结果

6.9. 带宽控制

配置端口带宽就是限制物理接口向外发送或向内接收数据的速率。

在流量从接口发出前，在接口的出方向上配置限速，对流出的所有报文流量进行控制。

在流量从接口接收前，在接口的入方向上配置限速，对流出的所有报文流量进行控制。

点击导航栏：配置 --> 带宽控制



图 59 带宽控制

6.9.1. 示例

将端口 1 出入口速率限制为 2048kbps，设置如下图。



图 60 带宽限制设置

在端口 1 连接 PC 上下载文件，打开任务管理器点击以太网显示接收速率为 2.1Mbps 如下图

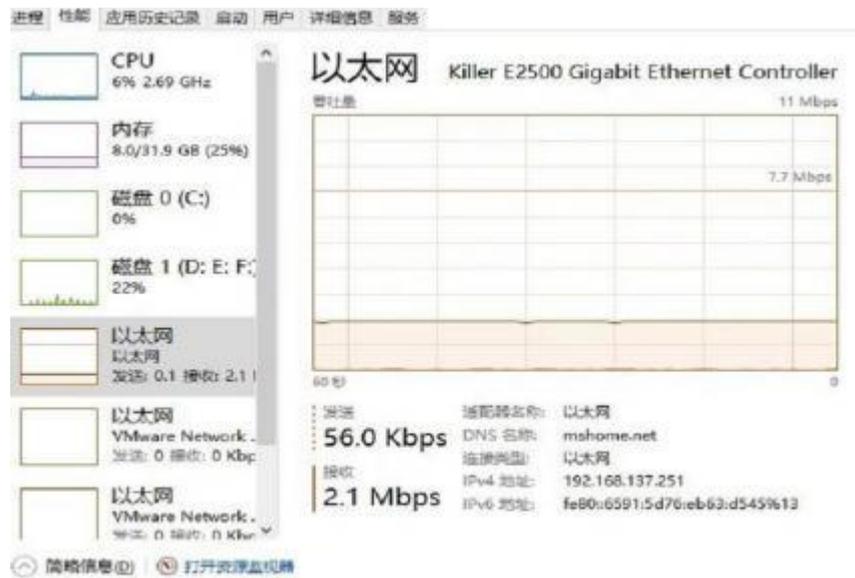


图 61 端口限速结果

6.10. 巨型帧

配置系统能转发的最大报文长度

点击导航栏：配置 --> 巨型帧



图 62 巨型帧

6.10.1. 示例

开启巨型帧后，设置 PC 网卡开启巨型帧，设置 ping 包数据 8000，不分包。命令 `ping -f 192.168.2.210 -l 8000 -t`，在 IP 为 192.168.2.210 的 PC 抓到巨型帧。

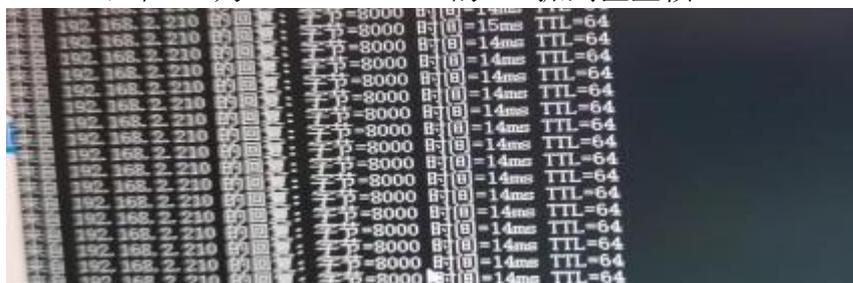


图 63 ping 大包

| | | | | | |
|-----------------|---------------|---------------|----------|--------------------------|---------|
| 14.. 171.5954.. | 192.168.2.210 | 192.168.2.100 | CS0 ICMP | 642 Echo (ping) reply | id=0x00 |
| 14.. 172.6010.. | 192.168.2.100 | 192.168.2.210 | CS0 ICMP | 8042 Echo (ping) request | id=0x00 |

图 64 抓到长度为 8042 的数据

6.11.MAC 约束

系统支持端口 Mac 学习限制功能。系统学习用户报文里的源 MAC，当学习到的 MAC 达到了限制阈值。如果用户报文的源 MAC 已经在 MAC 表中存在，用户报文将会继续转发；如果报文的源 MAC 不在 MAC 表中存在，系统会根据 MAC 限制动作对报文进行相应的处理。比如动作为丢弃，那么用户报文将在入端口丢弃。

点击导航栏：配置 --> Mac 约束



图 65 Mac 约束

6.11.1. 示例

没有设置 mac 地址约束时端口 2 学习到的 MAC 地址信息



图 66 端口 2 的 MAC 地址信息

将 2 端口 MAC 地址限制条目设置为 1 时，2 端口只能学习到一条 mac 地址信息



图 67 限制后端口 2 的 MAC 地址信息

6.12.绿色以太网

绿色以太网是指环保并降低设备功耗的功能。系统提供对电缆长度的连接和动态检测，以及对检测到的电缆长度所需的功率进行动态调整。高性能、低功耗。系统支持端口的 link down 省电，在断开网线时大大降低了功耗。当检测到输入信号后，从链路 down 省电中唤醒，进入正常模式。

点击导航栏：配置 --> 绿色以太网



图 68 绿色以太网

6.13.节能以太网 (EEE)

节能以太网(EEE)支持在低功耗空闲模式下运行。链路两端的系统可以在链路利用率低的时候禁用部分功能，从而节省功耗。建议关闭。

点击导航栏：配置 --> EEE



图 69 EEE 设置

6.14.SNMP

SNMP 是广泛应用于 TCP/IP 网络的网络管理标准协议，该协议能够支持网络管理系统，用以监测连接到网络上的设备是否有任何引起管理上关注的情况。SNMP 基本组件包括网络管理系统 NMS (Network Management System)、代理进程 (Agent)、被管对象 (Managed Object) 和管理信息库 MIB (Management Information Base)

点击导航栏：配置 --> SNMP



图 70 SNMP

6.14.1. 示例

1、打开 SNMP 功能



图 71 SNMP 使能

2、关闭管理 PC， 占用 162 端口的 SNMP 服务

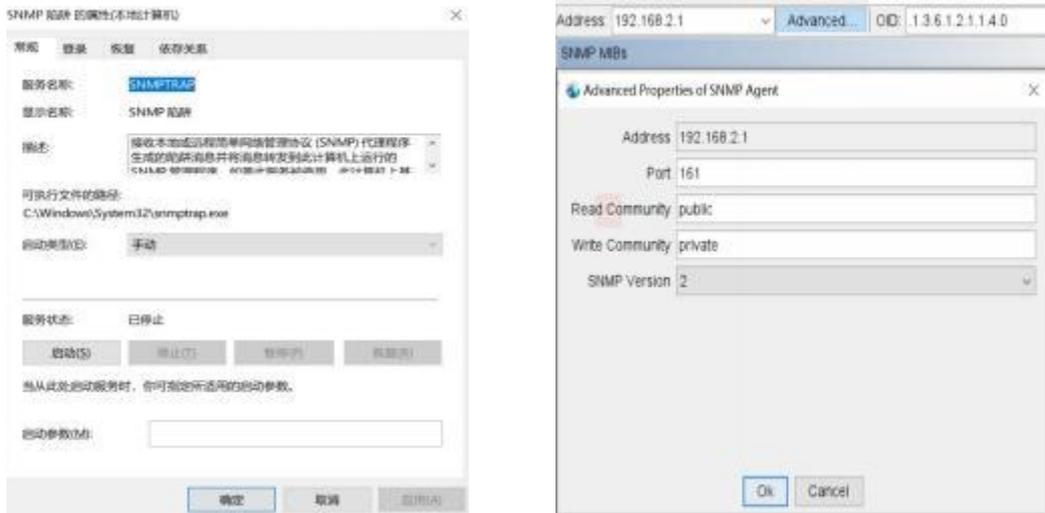


图 72 关闭管理主机 SNMP 服务及 MID Browser设置

3、打开 IReasoning MIB Browser 软件设置如上右图。

4、在 MIB Browser 点击 Get Next -> GO 显示结果如下图

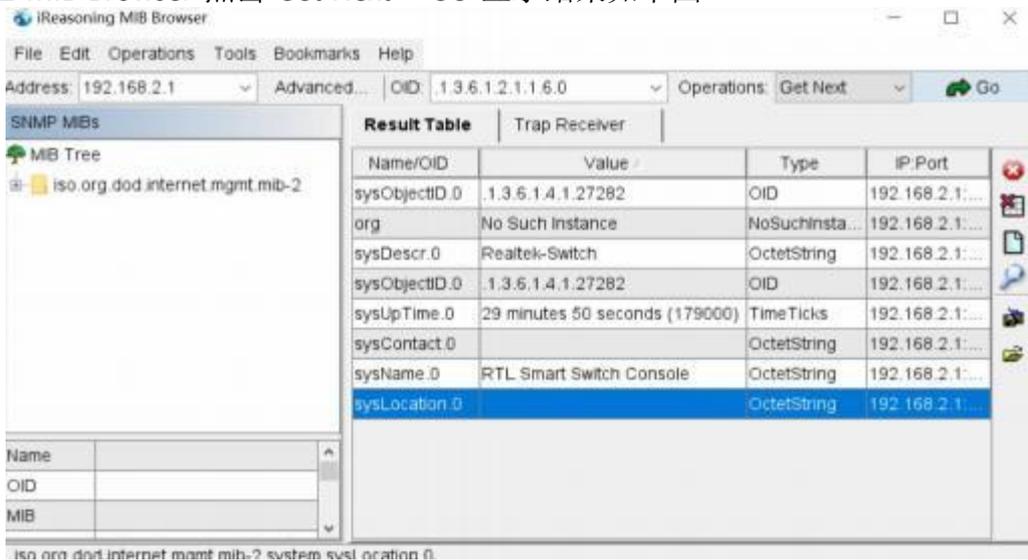


图 73 MIB Browser 显示

5、在 MIB Browser Operations 选择 set -> GO 后再 Get 结果显示如下。

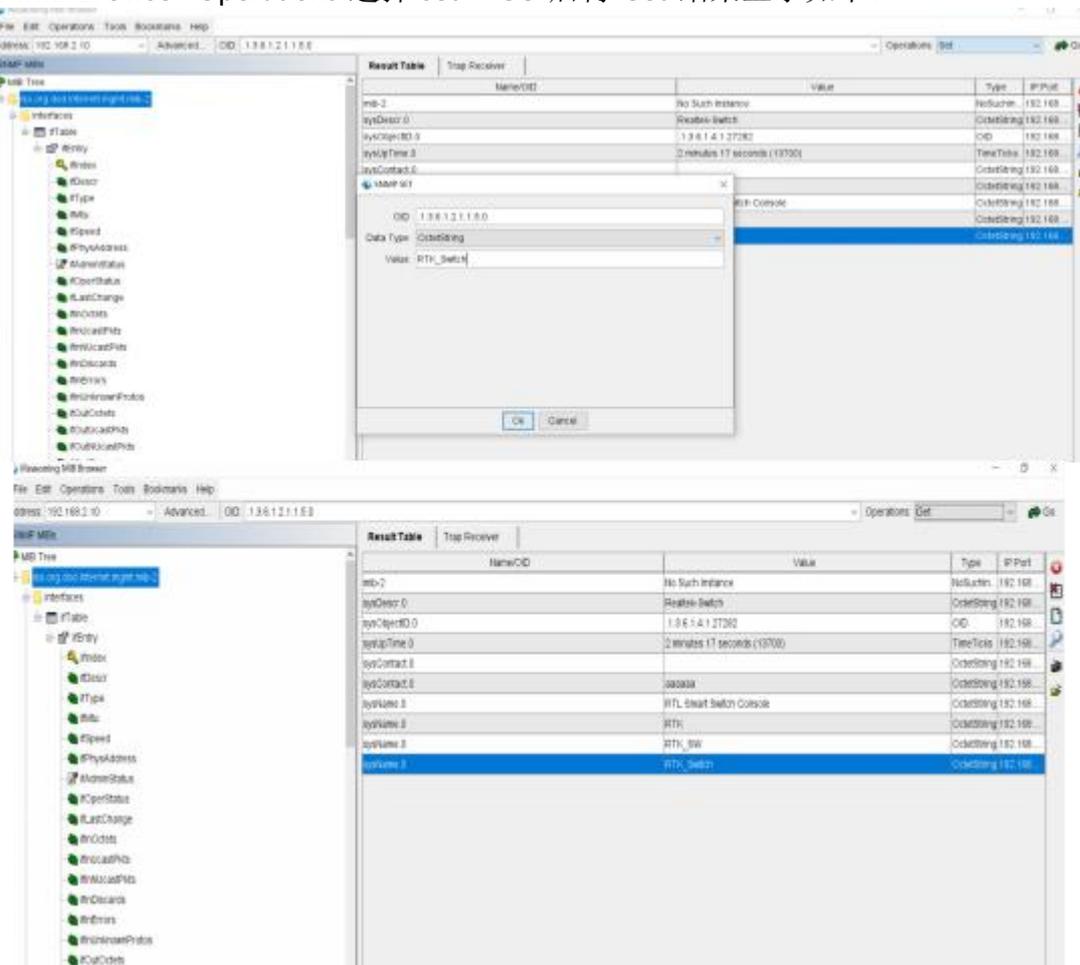


图 74 SNMP Trap Set

6、将管理 PC 的 IP 地址设置为交换机配置的 Trap IP 地址，在 MIB Browser Tools 选择 Trap Receiver 收到交换机端口状态变化信息

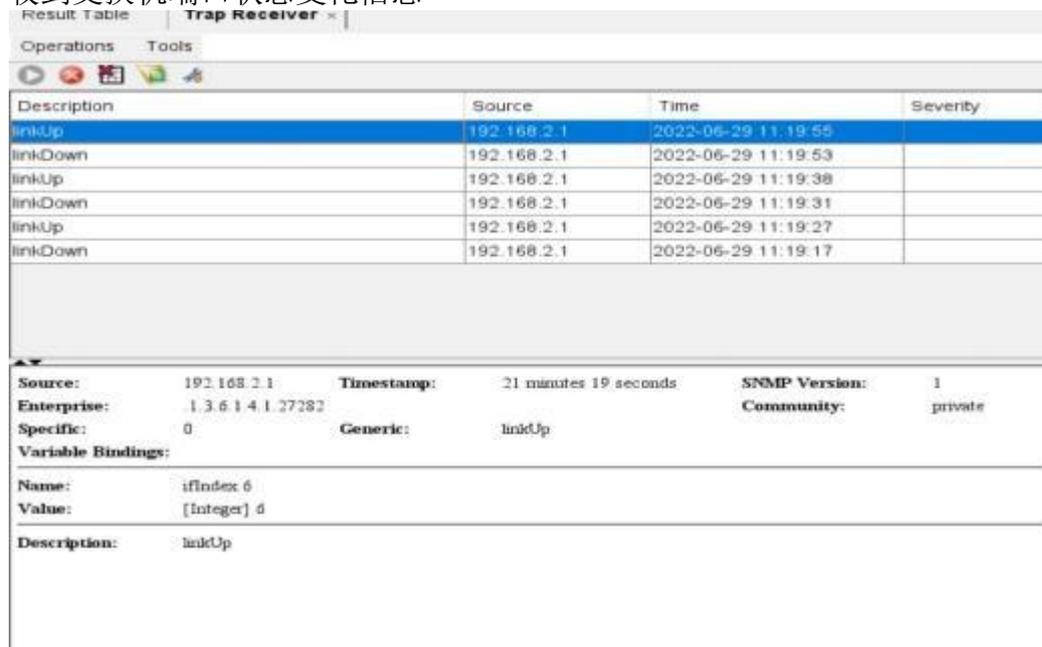


图 75 Trap Receiver

第七章 安全

7.1. MAC 地址

MAC 地址的英语是 Media Access Control Address，直译为媒体存取控制位址，也称为局域网地址（LAN Address）、以太网地址（Ethernet Address）或物理地址（Physical Address），它是一个用来确认网络设备位置的位址。

7.1.1. MAC 地址表

击导航栏：安全 --> MAC 地址 --> MAC 表

MAC地址信息

| No. | MAC 地址 | VLAN ID | 类型 | 端口 |
|-----|-------------------|---------|----|----|
| 1 | 00:E0:4C:68:12:CC | 1 | 动态 | 8 |
| 2 | 80:FA:5B:54:88:5C | 1 | 动态 | 1 |
| 3 | B0:25:AA:47:91:C7 | 1 | 动态 | 5 |

下一页

清除所有动态条目

图 76 MAC 地址信息

7.1.2. MAC 查找

击导航栏：安全 --> MAC 地址 --> MAC 查找

MAC地址搜索

| MAC 地址 | VLAN ID |
|-------------------|----------|
| 00:00:00:00:00:00 | (1~4094) |

查询

图 77 MAC 地址搜索

7.1.3. 静态 MAC

击导航栏：安全 --> MAC 地址 --> 静态 MAC

静态mac地址设置

| MAC地址 | VLAN ID | 端口 | 源MAC阻塞 |
|-------------------|----------|--|--------------------------|
| 00:00:00:00:00:00 | (1~4094) | <input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 | <input type="checkbox"/> |

Add

| No. | MAC地址 | VLAN ID | 端口 | 源MAC阻塞 | 选择 |
|-----|-------|---------|----|--------|----|
|-----|-------|---------|----|--------|----|

删除

图 78 静态 MAC

7.2. 广播风暴

广播风暴是指网络上的广播帧由于不断被转发导致数量急剧增加而影响正常的网络通讯，严重降低网络性能。广播风暴会占用相当可观的网络带宽，导致正常数据包无法正常运行。当广播数据充斥网络无法处理并占用大量网络带宽，导致正常业务不能运行，这就发生了广播风暴，造成局域网局部或整个网络瘫痪。

击导航栏：安全 --> 广播风暴

风暴抑制设置

| 风暴类型 | 端口 | 状态 | 速度 (kbps) |
|------|--|----|-------------|
| 广播 | <input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 | 关闭 | (8-1000000) |

应用

| 端口 | 广播 (kbps) | 组播 (kbps) | 未知单播 (kbps) | 未知组播 (kbps) |
|-----|-----------|-----------|-------------|-------------|
| 口 1 | 10000 | 10000 | 10000 | 10000 |
| 口 2 | 10000 | 10000 | 10000 | 10000 |
| 口 3 | 10000 | 10000 | 10000 | 10000 |
| 口 4 | 10000 | 10000 | 10000 | 10000 |
| 口 5 | 10000 | 10000 | 10000 | 10000 |
| 口 6 | 10000 | 10000 | 10000 | 10000 |
| 口 7 | 10000 | 10000 | 10000 | 10000 |
| 口 8 | 10000 | 10000 | 10000 | 10000 |

图 79 风暴抑制

说明：

风暴类型 广播、组播、未知单播，未知组播

端口 选择端口，可多选

状态 打开或关闭广播风暴抑制功能

速度 设置端口广播、组播包、未知单播、未知组播带宽。

第九章 工具

9.1. 固件升级

可以在此将交换机的软件升级。

击导航栏：工具 --> 固件升级



图 81 进入固件升级模式

点击<进入 loader模式> 按钮 出现下图

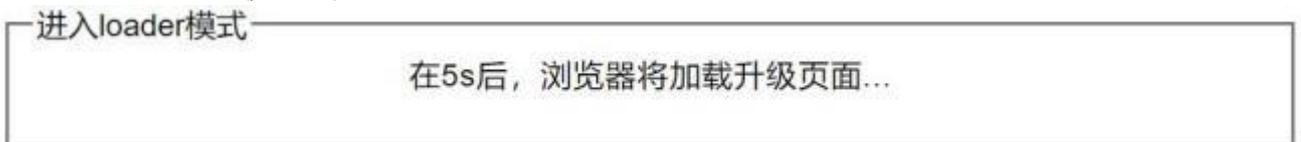


图 82 进入 loader 模式跳转

最后跳转到固件升级页面

点击导航栏 System --> HTTP Firmware Upgrade 出现如下图



图 83 固件升级页面

点击<选择文件> 按钮加载最新固件文件。再点击<Upgrade> 开始升级, 在弹出窗口点击<确定>。



升级完成后显示如下图。

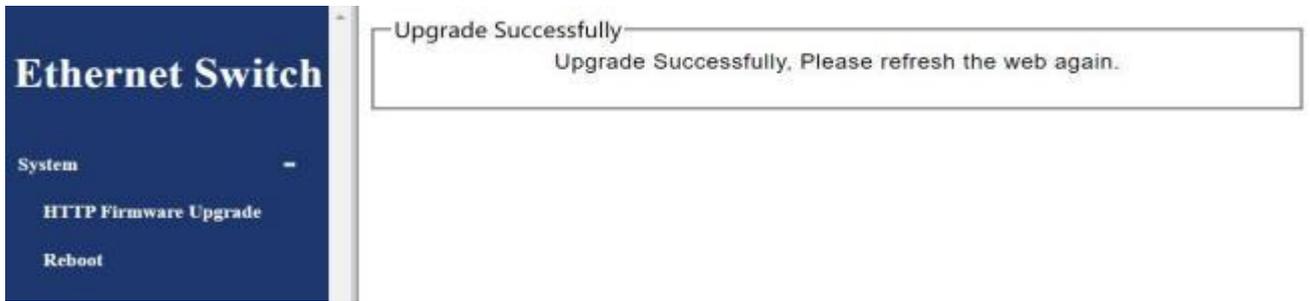


图 84 升级完成



注意：

固件升级过程中，请不要将设备断电，保持电源稳定，不要对页面进行刷新。升级固件可能会丢失当前未保存的配置信息，请在升级前保存配置。

击导航栏：System --> Reboot 可以重启交换机



9.2. 配置备份

可以在此保存当前的配置信息，建议在修改配置及升级软件前备份当前配置信息。

击导航栏：工具 --> 配置备份



图 85 配置备份和恢复

备份设置： 点击<备份> 通过浏览器将当前配置文件下载到本地。

恢复设置： 点击<选择文件> 选择配置文件，点击升级。之后重启交换机生效。

9.3. 复位

除了硬件恢复出厂设置开关，还可以在 Web 恢复默认设置。
点击导航栏：工具 --> 复位

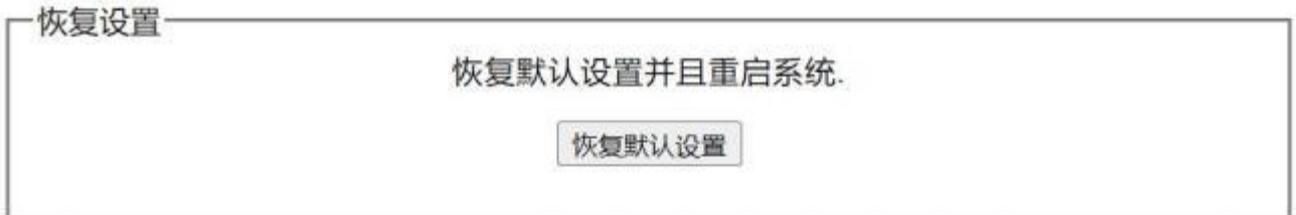


图 86 恢复默认设置

点击<恢复默认设置>按钮，交换机会恢复所有设置默认值。当前配置信息将会丢失。
建议在恢复默认值前，备份配置。

默认管理 IP 地址 192.168.2.1，账户名和密码均为 admin。

9.4. 保存

点击导航栏：工具 --> 保存

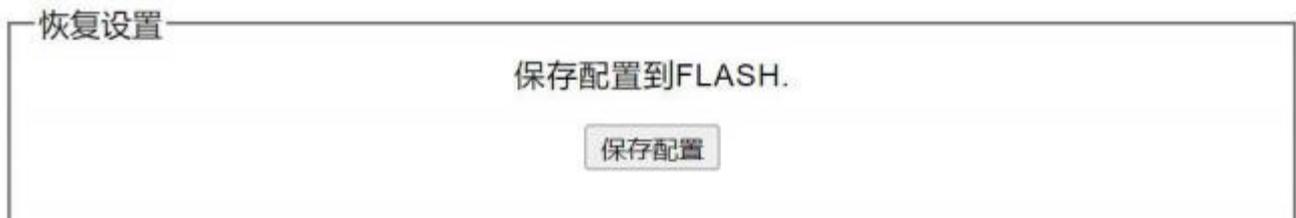


图 87 保存配置到 FLASH

建议修改设置后，保存设置到 FLASH。否则断电或重启修改的设置将会丢失。

9.5. 重启

点击重启后，交换机将重启，重启前建议保存配置，防止当前修改的配置丢失。
点击导航栏：工具 --> 重启

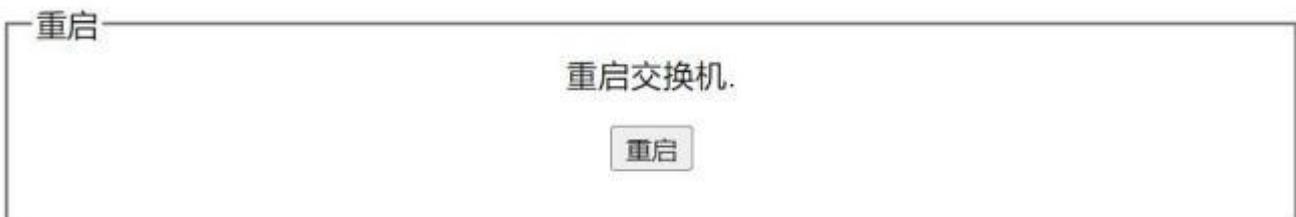


图 88 重启交换机



注意：

请不要在重启过程关闭电源，保证重启过程中电源稳定，避免强行断电。